FRAUD ALERT

NATIONAL CREDIT UNION ADMINISTRATION
1775 DUKE STREET, ALEXANDRIA, VA 22314

DATE: September 2009 **Fraud ALERT NO.: 09-Fraud-02**

TO: Federally Insured Credit Unions

SUBJ: Fraudulent Electronic Funds Transfers

Dear Board of Directors:

The National Credit Union Administration (NCUA) is alerting credit unions that provide or utilize web-based payment origination services of increased reports of fraudulent Electronic Financial Transactions (EFTs), such as ACH and wire transfers, resulting from compromised login credentials. Web-based EFT origination applications are being targeted by malicious software, including Trojan horse programs, key loggers, and others to circumvent online authentication methods. These types of malicious code can infect computers when visiting a website or opening an e-mail attachment and are difficult to detect because they lie dormant until the online banking session is initiated.

The implementation of information security best practices and comprehensive technology solutions is important to mitigate the risk of these and other potential intrusions. NCUA recommends credit unions implement the following controls:

- Strong Authentication – This requires appropriate authentication for web-based applications providing high-risk capabilities;
- Fraudulent Transaction Detection – This includes appropriate fraud detection and mitigation best practices such as transaction risk profiling;
- Out-of-Band Transaction Authentication – This entails using manual or transaction authentication systems in concert with fraud detection;
- Network Defense-in-Depth – This addresses having a best practice, layered Defense-in-Depth,[1] as part of the network and system infrastructure;
- Account Controls – This includes utilizing account features that protect accounts such as dual controls, transaction limits, time of day constraints; and

[1] Defense-in-depth is the coordinated use of multiple security countermeasures (i.e., firewalls, IDS, IPS, malware protection, access controls, etc.) to protect the integrity of the information assets in a credit union. The strategy is based on the principle that it is more difficult for a hacker or unauthorized individuals to defeat a complex and multi-layered defense system than to penetrate a single barrier.

- Secure Computers – This covers employing best practices to secure computers which perform high value or a large number of online transactions. These include properly hardening[2] and locking down computers.

Credit unions and technology service providers can refer to the following guidance for additional information:

LTCU 06-CU-13, Authentication for Internet Based Services – This letter provides guidance on the risk assessment process which should be utilized to determine the authentication solution is appropriate to process higher risk transactions.

LTCU 05-CU-20, Phishing Guidance for Credit Unions and Their Members – This letter highlights the need to educate your employees and members about phishing activities. Trojan horse, key loggers, and other spoofing techniques often result from phishing.

FFIEC Information Security Booklet – This booklet provides guidance on security strategy key concepts to assist in implementing a defense-in-depth security approach.

FFIEC Retail Payments Booklet – This booklet provides guidance on identifying and controlling risks associated with retail payment systems that process ACH and wire transfer transactions and related activities.

Credit unions are being attacked by malicious software in which perpetrators obtain their valid online banking credentials. The targets are vulnerable because:

- They do not have or do not use the most current authentication protocols;
- They lack sufficient authentication solutions for their higher risk transactions;
- They have not implemented sufficient transaction controls; and
- They have not implemented adequate reporting systems ("red flag" reporting).

Once a credit union or member's credentials are stolen, the perpetrator has online access to the account and any fund transfer capabilities associated with the credentials. These attacks could result in monetary losses to credit unions and their members if not detected quickly.

Sincerely,

/s/

Melinda Love
Director of Examination & Insurance

[2] Hardening is the process of securing a computer by reducing its surface of vulnerability. Hardening includes but is not limited to: applying updates to operating systems, applications, and malware software; limiting administrative and user accounts; utilizing personal firewalls to restrict network communication; utilizing strong log-on passwords; disabling unneeded features such as USB and CD/DVD drives; limiting and/or not permitting remote access; utilizing screensavers; and implementing Internet access controls.